FORTINET
High Performance Network Security

FortiWLM

Release 8.3.1

FortiWLM 8.3.1 release includes important fixes to be patched on the FortiWLM 8.3.0 GA and this release notes is to be used as an addendum to the 8.3.0 GA release notes.

To ensure a secured Wi-Fi network, Fortinet hardware (controllers and access points) are designed to run only the proprietary firmware developed by Fortinet. Only approved Fortinet access points are configurable with Fortinet controllers and vice versa. Third party access points and software cannot be configured on Fortinet hardware.

Fixed Issues

Bug ID	Description
0413853	Fixed infections reported by Microsoft Endpoint Protection when FortiWLM upgrade file is downloaded.

Common Vulnerabilities and Exposures

FortiWLM 8.3.1 is no longer vulnerable to the following CVE-Reference:

- 2017-7336
- Visit https://fortiguard.com/psirt for more information

Known Issues and Limitations

Bug ID	Description	Work Around
398408	WIPS UI not accessible in fresh install of FortiWLM for the first time.	Reboot FortiWLM server. After reboot, WIPS would be accessible.
423960	FortiWLC-SD 1000D/3000D 8.3.0 controllers cannot be upgraded from FortiWLM since SFTP is not supported on FortiWLC-SD	Upgrade using FortiWLC-SD GUI/CLI.

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

Contact

For assistance, contact Fortinet Customer Service and Support 24 hours a day at +1 408-542-7780, or by using one of the local contact numbers, or through the Support portal at https://support.fortinet.com/

Fortinet Customer Service and Support provide end users and channel partners with the following:

- Technical Support
- Software Updates
- Parts replacement service